UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,139	05/22/2001	Roy F. Quick JR.	010055B1	1058

23696 7590 11/24/2003

Qualcomm Incorporated
Patents Department
5775 Morehouse Drive
San Diego, CA 92121-1714

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 11/24/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Pl9

Office Action Summary	**Application No.** 09/863,139	**Applicant(s)** QUICK ET AL.
	Examiner Aravind K Moorthy	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *22 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) ☐ Notice of Informal Patent Application (PTO-152)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5, 7 .	6) ☐ Other: .

DETAILED ACTION

1. Claims 1-17 are pending in the application.

2. Claims 1-17 have been rejected.

Specification

3. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Local Authentication of Mobile Subscribers Outside their Home Systems.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1 and 5 are rejected under 35 U.S.C. 102(b) as being anticipated by Dean et al U.S. Patent No. 6,173,173 B1.

As to claim 1, Dean et al discloses a memory and a processor configured to implement a set of instructions stored in the memory [column 3, line 17-33]. Dean et al discloses generating a plurality of keys in response to a received challenge [column 15 line 54 to column 16 line 35]. Dean et al discloses generating an initial value based upon a first key from the plurality of keys [column 16, lines 15-35]. Dean et al discloses concatenating the initial value with a received signal to form an input value [column 16, lines 15-35]. Dean et al discloses that the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module [column 16, lines 15-35]. Dean et al discloses that the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit [column 16, lines 15-35]. Dean et al discloses hashing the input value to form an authentication signal [column 16, lines 60-67]. Dean et al discloses transmitting the authentication signal to the communications system via the communications unit [column 16, lines 15-35].

As to claim 5, Dean et al discloses receiving the second key from the subscriber identification module [column 13 line 35 to column 14 line 16]. Dean et al discloses generating a local initial value based upon the second key [column 13 line 35 to column 14 line 16]. Dean et al discloses concatenating the local initial value and a message to form a local input value [column 16, lines 15-35]. Dean et al discloses hashing the local input value to form the received signal [column 16, lines 15-35]. Dean et al discloses transmitting the received signal to the subscriber identification module [column 16, lines 15-35].

5. Claims 8-13, 15 and 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Reeds, III U.S. Patent No. 5,204,902.

As to claim 8, Reeds et al discloses a key generation element [column 4, lines 32-46]. Reeds et al discloses a signature generator configured to receive a secret key from the key generation element and information from a mobile unit [column 5, lines 24-34]. Reeds et al discloses generating a signature that will be sent to the mobile unit [column 6, lines 3-35]. Reeds et al discloses that the signature is generated by concatenating the secret key with the information from the mobile unit and hashing the concatenated secret key and information [column 6, lines 24-35].

As to claim 9, Reeds et al discloses that the generation element comprises a memory and a processor configured to execute a set of instructions stored in the memory [column 4, lines 27-31]. Reeds et al discloses that the set of instructions performs a cryptographic transformation upon an input value to produce a plurality of temporary keys [column 4, lines 32-46]].

As to claim 10, Reeds et al discloses that the cryptographic transformation is performed using a permanent key [column 4, lines 27-31].

As to claim 11, Reeds et al discloses a key generator for generating a plurality of keys from a received value and a secret value [column 4, lines 32-46]. Reeds et al discloses that at least one communication key from the plurality of keys is delivered to the communications unit and at least one secret key from the plurality of keys is not delivered to the communications unit [column 7 line 41 to column 8 line 60]. Reeds et al discloses a signature generator for generating an authorization signal from hashing a version of the at least one secret key together with an authorization message [column 6, lines 36-67]. Reeds et al discloses that the authorization message is generated by the communications unit using a version of the at least one communication key [column 6, lines 36-67].

As to claim 12, Reeds et al discloses that the subscriber identification module is configured to be inserted into the communications unit [column 4, lines 27-31].

As to claim 13, Reeds et al discloses that at least one communication key comprises an integrity key [column 4, lines 27-31].

As to claim 15, Reeds et al discloses generating a plurality of keys, as discussed above. Reeds et al discloses transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys [column 4, lines 27-31]. Reeds et al discloses generating a signature at the communications device using both the at least one key transmitted to the communications device and a transmission message, as discussed above. Reeds et al discloses that generating is implemented by hashing a concatenated value formed from the at least one key and the transmission message, as discussed above. Reeds et al discloses transmitting the signature to the subscriber identification device [column 6, lines 36-67]. Reeds et al discloses receiving the signature at the subscriber identification device [column 7, lines 35-67]. Reeds et al discloses generating a primary signature from the received signature [column 6, lines 36-67]. Reeds et al discloses that the generating is implemented by hashing a concatenated value formed from the at least one private key and the signature received from the communications device [column 6, lines 36-67]. Reeds et al discloses conveying the primary signature to a communications system [column 6, lines 36-67].

As to claim 17, Reeds et al discloses a memory and a processor configured to implement a set of instructions stored in the memory, as discussed above. Reeds et al discloses that the set of instructions for selectively generates a primary signature based upon a key that is held private from the mobile station and a secondary signature that is received from the mobile station, as discussed above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dean et al U.S. Patent No. 6,173,173 B1 as applied to claim 1 above, and further in view of Applied Cryptography (hereinafter Schneier).

As to claim 2, Dean et al discloses using hash functions, as discussed above.

Dean et al does not teach that the hash function is the Secure Hash Algorithm (SHA-1).

Schneier teaches the Secure Hash Algorithm (SHA-1) and its benefits [pages 442-445].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dean et al so that the hashing function was the Secure Hash Algorithm (SHA-1).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dean et al by the teaching of Schneier because there are no known cryptographic attacks against SHA and it is more resistant to brute-force attacks [page 445].

7. Claims 3, 4, 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dean et al U.S. Patent No. 6,173,173 B1 as applied to claim 1 above, and further in view of Deindl et al U.S. Patent No. 6,076,162.

As to claims 3, 4, 6 and 7, Dean et al does not teach that generating the initial value comprises padding the first key. Dean et al does not teach that generating the initial value further comprises adding the padded first key bit-wise to a constant value. Dean et al does not teach that generating the local initial value comprises padding the second key. Dean et al does not teach that generating the local initial value further comprises adding the padded second key bit-wise to a second constant value.

Deindl et al teaches padding a key and adding the padded key bit-wise to a constant value.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dean et al so that the initial values would have been generated by padding the first and second key and adding both of the padded keys to a constant value.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dean et al by the teaching of Deindl et al because data can be extended to fill up any necessary block length [column 4, lines 46-56].

8. Claims 14 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, III U.S. Patent No. 5,204,902 as applied to claims 11 and 15 above, and further in view of Applied Cryptography (hereinafter Schneier).

As to claims 14 and 16, Reeds discloses using hash functions, as discussed above.

Reeds does not teach that the hash function is the Secure Hash Algorithm (SHA-1).

Schneier teaches the Secure Hash Algorithm (SHA-1) and its benefits [pages 442-445].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reeds so that the hashing function was the Secure Hash Algorithm (SHA-1).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Reeds by the teaching of Schneier because there are no known cryptographic attacks against SHA and it is more resistant to brute-force attacks [page 445].

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-1373.

Aravind K Moorthy
November 18, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100